



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003233521 A
 (43) Date of publication of application: 22.08.2003

(51) Int. Cl. G06F 12/00
 G06F 11/00, G06F 12/14

(21) Application number: 2002034804
 (22) Date of filing: 13.02.2002

(71) Applicant: HITACHI LTD
 (72) Inventor: ARAI MASATO
 UMETSU TOSHIKAZU

(54) FILE PROTECTION SYSTEM

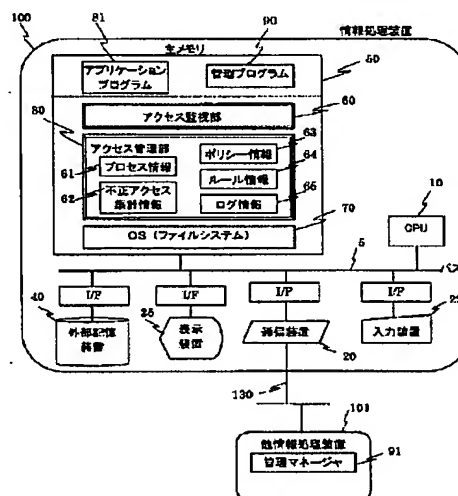
COPYRIGHT: (C)2003,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a file protection system capable of detecting illicit access regarded to be malicious by the monitoring result of file access in real time for prohibiting the illicit access and preventing illicit operation caused afterward.

SOLUTION: Among file accesses monitored by an access monitoring part 60, an access management part 80 rejects a file access violating access policy information 63, and at the same time, the access is recorded as abnormal access summarization information 62. If the summarization information satisfies a criterion defined by rule information 64, it is regarded that there exists an illicit access having malicious intention, and protection processing defined by the rule information 64 is carried out by the access management part 80 for preventing the following illicit operation.

図 1



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-233521
(P2003-233521A)

(43) 公開日 平成15年 8 月22日 (2003. 8. 22)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 Z 5 B 0 1 7
11/00		12/14	3 1 0 K 5 B 0 7 6
12/14	3 1 0		3 2 0 A 5 B 0 8 2
	3 2 0	9/06	6 6 0 N

審査請求 未請求 請求項の数13 O L (全 17 頁)

(21) 出願番号 特願2002-34804(P2002-34804)

(22) 出願日 平成14年 2 月13日 (2002. 2. 13)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 荒井 正人

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 梅都 利和

愛知県尾張旭市晴丘町池上 1 番地 株式会

社日立製作所情報機器事業部内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

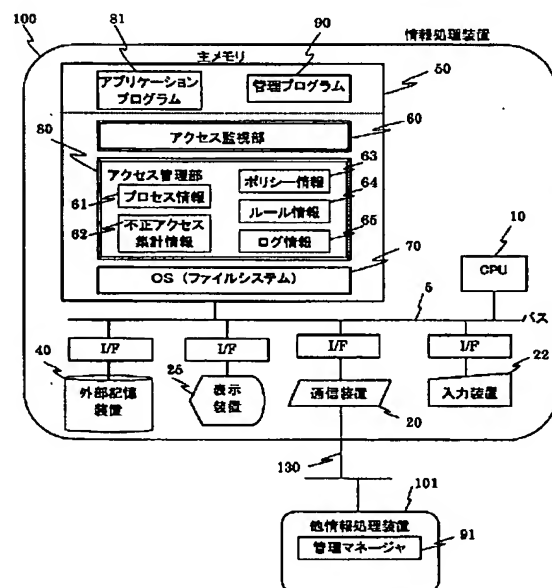
(54) 【発明の名称】 ファイル保護システム

(57) 【要約】

【課題】 ファイルアクセスの監視結果から悪意があると思われる不正アクセスをリアルタイムに検出し、当該アクセスを禁止すると共に、以後発生する不正行為まで阻止可能なファイル保護システムを提供する。

【解決手段】 アクセス監視部 6 0 が監視するファイルアクセスのうち、ポリシー情報 6 3 に違反したものをアクセス管理部 8 0 により阻止すると同時に、異常アクセス集計情報 6 2 にて記録する。上記集計情報がルール情報 6 4 にて規定した判定基準を満たした場合には、悪意をもつ不正アクセス主体が存在すると見なして、同じくルール情報 6 4 にて定義された防御処理をアクセス管理部 8 0 により実行し、以後の不正行為を防止する。

図 1



【特許請求の範囲】

【請求項 1】ファイルシステムを備えた情報処理装置において、
ファイルアクセスの監視および制御処理を行うアクセス制御手段と、
正常アクセスと異常アクセスを区別するためのポリシー情報と、
異常アクセスのなかから不正アクセスを区別するための判定基準を備え、
前記アクセス制御手段は、
前記ポリシー情報を用いて異常アクセスを検出する手段と、
前記判定基準を用いて不正アクセスを検出する手段と、
前記異常アクセスと不正アクセスの実行を防止する手段を備えるファイル保護システム。
【請求項 2】請求項 1 のファイル保護システムにおいて、
前記異常アクセス検出手段と、前記不正アクセス検出手段とが検出した異常アクセスおよび／または不正アクセスについて証拠を記録する手段を備えるファイル保護システム。
【請求項 3】請求項 1 のファイル保護システムにおいて、
前記アクセス制御手段は、第 1 段階として、前記異常アクセス検出手段を用いて異常アクセスを検出し、第 2 段階として、前記不正アクセス検出手段を用いて異常アクセスの中から不正アクセスを検出するファイル保護システム。
【請求項 4】請求項 3 のファイル保護システムにおいて、
前記ポリシー情報は、正常なアクセスを定義し、および／または、
前記判定基準は、不正アクセスを検出するため、不正アクセスを定義した不正アクセス判定基準であるファイル保護システム。
【請求項 5】請求項 4 のファイル保護システムにおいて、
さらに、前記不正アクセス判定基準を満たした場合に実行すべき防御処理を定めたルール情報を備え、
前記アクセス制御手段は、
前記不正アクセス検出手段が不正アクセスを検出した場合に、前記ルール情報に従い前記防御処理を実行する防御処理手段を備えるファイル保護システム。
【請求項 6】請求項 5 のファイル保護システムにおいて、
前記ポリシー情報は、記憶装置名、ボリューム名、ドライブ名、ディレクトリ名、ファイル名のいずれか、あるいはそれらの組み合わせで表記された保護対象の名称と、当該保護対象に対する正常なアクセスの条件を記述したものであるファイル保護システム。

【請求項 7】請求項 6 記載のファイル保護システムであって、
前記ポリシー情報はさらに、当該保護対象の重要度を記述したものであり、
前記不正アクセス判定基準において、保護対象の重要度 L と、異常アクセス回数 N と、有効期間 T とを指定し、
前記重要度 L を割り当てられた 1 つ以上の保護対象に対して、前記有効期間 T 内に、前記異常アクセスが前記 N 回以上発生した場合を不正アクセスと定義するファイル保護システム。
【請求項 8】請求項 6 記載のファイル保護システムであって、
前記不正アクセス判定基準において、保護対象の名称 F と、異常アクセス回数 N と、有効期間 T とを指定し、前記名称 F の保護対象に対して、前記有効期間 T 内に、前記異常アクセスが前記 N 回以上発生した場合を、不正アクセスと定義するファイル保護システム。
【請求項 9】請求項 5 記載のファイル保護システムであって、
前記ポリシー情報を複数備え、
前記防御処理手段は、
前記ポリシー情報の切り替え処理手段と、管理者への通知処理手段と、複数の防御処理の中から 1 つ以上の処理を実行する手段を備えるファイル保護システム。
【請求項 10】請求項 6 記載のファイル保護システムであって、
前記アクセス制御手段は、さらに、実行中のプログラムの監視処理手段を備え、
前記不正アクセス判定基準において、異常アクセス回数 N と、有効期間 T とを指定し、前記有効期間 T 内に、同一の実行中プログラムから、前記異常アクセスが前記 N 回以上発生した場合を、不正アクセスと定義するファイル保護システム。
【請求項 11】請求項 9 記載のファイル保護システムであって、
前記防御処理手段は、さらに、前記実行中プログラムの処分手段を備え、
前記実行中プログラムの処分手段は、
前記実行中プログラムによる以後のアクセスを禁止するアクセス禁止処理手段と、
前記実行中プログラムを終了させる強制終了処理手段と、
前記実行中プログラムによる以後のアクセスを全てダメージファイルへのアクセスに変換して当該アクセスを監視および／または記録する監視記録処理手段と、
前記アクセス禁止処理手段、前記強制終了処理手段、または前記監視記録処理手段のいずれかを実行する手段を備えるファイル保護システム。
【請求項 12】請求項 3 記載のファイル保護システムであって、

当該ファイル保護システムの管理者に、不正なアクセスの発生状況を提供する手段と、

前記管理者から実行中プログラムの強制終了処理、ポリシー切り替え処理、ルール設定処理から任意の処理の実行指示を受け付ける手段を備えるファイル保護システム。

【請求項13】請求項1記載のファイル保護システムにおいて、

前記アクセス制御手段は、さらに、プログラムの起動の監視手段を備え、

前記ポリシー情報は、前記情報処理装置にて利用可能なプログラムの名称と、当該プログラムからの正常なアクセスの条件を定義し、

前記アクセス制御手段は、

プログラムの起動を検知して前記ポリシー情報と照合し、前記ポリシー情報に登録されていないプログラムの起動であった場合に当該プログラムの起動を防止する処理手段と、

当該プログラムが、前記ポリシー情報に登録されているプログラムであった場合には、当該プログラムからのファイルアクセスを前記ポリシー情報と照合し、適合したファイルアクセスの実行を許可する手段を備えるファイル保護システム

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータシステムが管理する情報資産を不正なアクセスから保護する場合に好適なファイル保護方法に関する。

【0002】

【従来の技術】情報ネットワークシステムにて発生し得るセキュリティ脅威は、ネットワークを経由して外部から攻撃するケースと、情報資産が格納されたホストを内部にて直接操作して攻撃するケースとに大別できる。このような攻撃から情報資産を保護する策として、ファイアウォールによるネットワークレベルのアクセス制御機能や、ホストに搭載したOS(Operating System)が備えるファイルアクセス制御機能を用いるのが一般的である。また、攻撃に用いられるパケットの既知の特徴(プロトコルヘッダー中のポート番号や、データ部分の内容など)を用いたパターン照合により、ネットワーク上のパケットを分析し、不正アクセスと思われるパケットを検出してアラームを発したり、ファイアウォールやルータの設定を変更したりすることにより、不正と思われる通信を積極的に検出し、その場で遮断するといった不正アクセス監視技術もある。更に、どのようなパケットが通過したのかをログ情報として記録、保存しておくことで、後日問題が発覚した場合に追跡調査も可能となる。

【0003】不正行為の目的には様々なものがあると予想できるが、情報ネットワークシステムにおいて最も重要な保護対象は、ファイルやデータベースに格納された

情報資産であることから、不正行為を阻止するためには、情報資産に対する直接的なアクセスも監視し、不正なアクセスの検知と防御ができることが望まれる。このような技術には、前述のようにOSが備えるファイルアクセス制御機能が代表的なものとして挙げられる。

【0004】これは、予め各ファイルに対する正常なアクセスを、情報資産(ファイル名)と、アクセスタイプ(read, write, execute)と、アクセス元(ユーザー名、グループ名)を組み合わせたパーミッション情報として定義しておき、正常でない、つまり異常なアクセスを遮断するものである。また、ファイルへのアクセスを監視し、異常なアクセスを検出すると当該ファイルのパーミッション情報を変更する方法が、米国特許5919258号に開示されている。

【0005】

【発明が解決しようとする課題】先に述べた異常アクセスは、不用意(過失)によるものと故意(悪意)によるものとに大別できる。上記特開平9-218837号公報にて開示しているファイルアクセスの監視方法では、異常なファイルアクセスを1度でも検出するとアクセスパーミッションを変更するため、正規のユーザーによる誤ったファイル操作であっても、例えば共有ファイルが他のユーザーから一時的に利用できなくなる可能性がある。つまり、ファイル保護の観点からは有効であるが、不用意なファイルアクセスによって通常業務に支障をきたす点で問題がある。

【0006】一方、異常なファイルアクセスを発行したアクセス主体(実行中のプログラムまたはプロセス)が、真に悪意をもつものであれば、ファイルアクセス以外にもどのような不正行為を働くか予想できない。このような異常なファイルアクセスを試みた実行中プログラム(プロセス)を放置しておく、やがてOSやプログラムに潜在するセキュリティホールを発見し、監視の目を潜り抜け、悪意を持ってアクセスしてくる恐れもある。

【0007】従って、改善されたファイル保護システムが望まれている。

【0008】

【課題を解決するための手段】本発明は、ファイルアクセスを監視し、その結果から悪意の有無を判断するファイル保護システムを提供する。

【0009】さらに、悪意があると判断するアクセスを検出した場合、当該アクセスを禁止すると共に、以後発生する不正行為を阻止するための防御処理を実行するファイル保護システムを提供する。これにより、情報資産をより安全に利用することが可能になる。

【0010】通信を例にとって説明した、従来の不正アクセス監視技術は、通信データや通信量、アプリケーションで使用されるコマンドといった情報から不正と思われる行為の有無を検知するものであり、その行為が真に

不正なものかどうかまでを監視するものではない。これに対し、本発明によるファイル保護システムは、さらに、上記異常なファイルアクセスを発行したアクセス主体が働くかもしれない不正行為に対して先手を打つために、上記アクセス主体そのものの行為を制限するファイル保護システムを提供する。

【0011】なお、本明細書においては、正常なアクセスではないアクセスを「異常アクセス(unauthorized access)」といい、異常アクセスの内、悪意によるアクセスを「不正アクセス(malicious access)」という。

【0012】本発明のファイル保護システムは、正常アクセスと異常アクセスを区別するためのアクセス制御ポリシー情報(ポリシー情報という)と、不正アクセスとそうではない異常アクセスを区別するための判定基準を備える。より具体的に、アクセス制御ポリシー情報は正常なアクセスを定義するものであって良い。判定基準は、不正アクセスを検出するための不正アクセス判定基準であって良い。

【0013】本発明のファイル保護システムは、第1段階として、ポリシー情報を用いて異常アクセスを検出し、第2段階として不正アクセス判定基準を用いて異常アクセスの中から不正アクセスを検出する。

【0014】本発明のファイル保護システムによれば、ファイルシステムを備えた情報処理装置は、ファイルアクセスの監視と制御処理を行うアクセス制御部と、正常なアクセスを規定したアクセス制御ポリシー情報と、悪意のある行為かどうかを判断するための不正アクセス判定基準、および当該基準を満たした場合に実行すべき処理について記述したルール情報とを備える。上記アクセス制御部は、上記情報処理装置におけるファイルアクセスの監視結果が、上記ルール情報に記述された不正アクセス判定基準に達した場合に、同じく上記ルール情報に記述された所定の処理を実行することにより、上記ファイルアクセスの要求元となるプログラムからの以後のアクセスを制限することを特徴とする。

【0015】上記アクセス制御ポリシー情報は、保護対象となるファイルの名称およびその重要度と、当該ファイルに対する正常アクセスの条件を記述したものであり、当該正常アクセスの条件を満たさないアクセスを上記アクセス制御手段が検出した場合は、当該アクセスを異常アクセスとみなす。

【0016】上記ルール情報に記述する不正アクセス判定基準は、例えば保護対象となるファイルの重要度と、当該重要度が割り当てられたファイルに対して許容できる異常アクセスの回数Nを規定したものであり、これにより、重要なファイルに対して異常アクセスが上記N回以上試みられた場合に悪意のあるアクセスであると判断する。あるいは、特定の同一ファイルに対する異常アクセスが上記N回以上試みられた場合に悪意のあるアクセスと判断してもよいし、更に他の基準として、同一のア

クセス主体から異常なアクセスが上記N回以上試みられた場合に悪意のあるアクセスと判断してもよい。

【0017】上記不正アクセス判定基準を満たした場合に実行すべき処理として、例えば、不正アクセスの要求元となる実行中のプログラムを強制的に終了させる旨を、上記ルール情報に記述する。これにより、重要なファイルに対して上記N回以上の異常なアクセスを試みたプログラムは、上記アクセス制御手段により強制的に終了される。

【0018】また上記、不正アクセスの要求元となる実行中のプログラムからの以後のアクセスに対して、全てエラーを返す旨を、上記ルール情報に記述してもよい。これにより、重要なファイルに対して上記N回以上の異常なアクセスを試みたプログラムは、以後、発行するファイルアクセスは全て上記アクセス制御手段がエラーを返すことで却下される。

【0019】また上記不正アクセスの要求元となる実行中のプログラムからの以後のアクセスを全てダミーファイルへのアクセスにリダイレクトし、当該ダミーファイルへのアクセスを監視・記録する旨を、上記ルール情報に記述してもよい。これにより、重要なファイルに対して上記N回以上の異常なアクセスを試みたプログラムからは、以後、発行するファイルアクセスが全て正常に処理されたようにみえるが、実際にはダミーファイルへのアクセスであるため、重要なファイルには被害が及ばない。

【0020】また、上記アクセス制御ポリシーを切り替える旨を、上記ルール情報に記述してもよい。これにより、重要なファイルに対して上記N回以上の異常なアクセスが発生した場合、上記アクセス制御部は所定のアクセス制御ポリシーに切り替えて、以後のファイルアクセスをコントロールする。このとき、切り替え後のアクセス制御ポリシーを、切り替え以前のポリシーよりも制限の厳しいものとすることで、以後のファイルアクセスの正当性をより厳重にチェック可能となる。

【0021】本発明のファイル保護システムによれば、上記ルール情報には、不正アクセス判定基準と当該基準を満たした場合に実行すべき処理との組み合わせ情報を、保護対象となるファイルの種類や重要度に応じて異なるものを指定することもできる。

【0022】また、本発明を実現するのに必要な各プログラム(コード、モジュール、ユニットともいう)は、ネットワークに接続される他のサーバからコンピュータが読み取り可能な媒体、すなわちネットワーク上の伝送信号、またはCD-ROM、FDなどの可搬型記憶媒体、を経由して、事前にまたは必要ときに導入してもよい。

【0023】

【発明の実施の形態】以下、図を用いて本発明の実施の一形態を説明する。図1に、本発明の一実施形態が適用

された情報処理装置の構成を示す。情報処理装置100は、CPU10、通信装置20、入力装置22、表示装置25、外部記憶装置40、主メモリ50、バスなどの内部信号線5から構成され、アプリケーションプログラム81などから上記外部記憶装置40へのアクセスは、全てアクセス監視部60によって監視されており、アクセス管理部80による権限チェックを受け、許可された場合に限りOS70を介して処理される。上記アクセス管理部80は、ポリシー情報63、プロセス情報61、ルール情報64、ログ情報65、異常アクセス集計情報62を用いて、アクセス権チェック処理や不正アクセス防止策を実行する。上記外部記憶装置40の記録媒体としては、ハードディスク、CD-ROM、FD、MO、テープデバイスなどであってよい。また、これらの記憶媒体は、外部記憶装置40に固定されたものでもよいし、可搬型であってもよい。また、外部記憶装置40そのものが、独立したネットワークを構築したストレージ・エリア・ネットワーク(SAN)であってもよい。

【0024】ポリシー情報63は、上記外部記憶装置40内のデータに対する正常アクセスを定義したものである。プロセス情報61は、現在実行中のプログラムに関する情報を格納したテーブルである。ルール情報64は、異常なファイルアクセスのうち、悪意による不正アクセスを判別するための判定基準と、悪意による不正アクセスが発生したと判定した際に上記アクセス管理部80がとるべき処理について規定したものである。ログ情報65は、上記アプリケーションプログラム81から上記外部記憶装置40内のデータへのアクセスに関する証拠や、各種イベントに関する証拠を記録するためのものである。異常アクセス集計情報62は、過去に発生したポリシー違反のアクセスに関する情報をリアルタイムに集計したものである。

【0025】管理プログラム90は、管理者により上記の各種情報61～65の参照や書き込み処理を行うために利用されるものである。管理プログラム90は、上記アクセス管理部80を経由して上記各種情報61～65にアクセスする。

【0026】なお、上記OS70は、ファイルシステムを標準で装備している基本ソフトウェアであり、本実施形態のファイル保護システムは、アクセス監視部60と、アクセス管理部80と、上記各種情報61～65と、管理プログラム90から構成される。つまり、少なくともファイルシステムを備えた情報処理装置であれば、本実施形態のファイル保護システムの適用は可能である。

【0027】また、上記アプリケーションプログラム81は、例えばワープロソフトや、ブラウザ、インターネットサーバプログラムなど、多種多様なプログラムを意味している。上記OS70と、アクセス監視部60と、アクセス管理部80と、アプリケーションプログラム8

1と、管理プログラム90は、それぞれ外部記憶装置40またはネットワーク130を介して他の情報処理装置101から上記主メモリ50にロードされ、実行するのである。ただし、ファイル保護システムが実行開始する前に、アプリケーションプログラムがファイルアクセスを実行することを避けるため、OSが最初にロードされ、アプリケーションプログラム81や管理プログラム90よりも先に、アクセス監視部60や、アクセス管理部80がロードされる。このようなロードの順序は、OSによってコントロールできる。

【0028】以下では、上記OS70がユーザーの識別・認証機能を備えており、上記アプリケーションプログラム81は、上記機能により識別・認証されたユーザーの名義でファイルアクセスを実行するとの仮定のもとで、本発明の実施の一形態を示す。

【0029】図2に、上記ポリシー情報63の構成を示す。ポリシー情報63は、ポリシーインデックス200と、システムポリシー210と、ユーザーポリシー220と、エラーコード表230から構成される。ポリシーインデックス200は、複数あるポリシーの識別情報と、現在有効なポリシーを索引するために必要な情報を格納したものである。

【0030】システムポリシー210と、ユーザーポリシー220は、どちらも外部記憶装置内のファイルに対する正常なアクセスを定義したものであるが、システムポリシーとは、いかなる場合にも共通的なポリシーを記述したものであり、ユーザーポリシーとは、例えば「運用モード」「保守モード」「非常モード」のような情報処理装置100の用途や状況に応じて、個別に記述されたポリシーである。したがって、ユーザーポリシーは、予めいくつかのモード毎にポリシーを登録しておき、適宜切り替えながら上記アクセス管理部80がアクセス権をチェックすることが望ましい。

【0031】エラーコード表230は、上記システムポリシーやユーザーポリシーのいずれかに違反したアクセスを発行したアプリケーションプログラム81に対して、アクセス管理部80からアクセス監視部60を経由して返すべきエラーコードを記述したものである。

【0032】図3に、上記ポリシーインデックスの一例を示す。ポリシーインデックス200は、デフォルトのポリシーを識別するためのデフォルトフラグ301と、現在有効なポリシーを識別するための有効フラグ302と、ポリシーの識別番号303と、ポリシー名称304、各ポリシーの記載箇所を表すロケーション情報305からなる。上記デフォルトフラグ301は、有効フラグの初期値でもある。また、システムポリシーは常に有効でなければならないことから、デフォルトフラグ、有効フラグ共に「1」である。

【0033】図4に、ポリシーの一例を示す。前述のように、ポリシーはシステムポリシー210とユーザーポ

リシー 220 とに大別できるが、記述形式は共通であり、保護対象の名称 401 と、その重要度 402、アクセスタイプ 403、プログラム名 404、特徴値 405、ユーザー名 406、時間 407 から構成される。上記アクセスタイプ 403 には、Read (読み出し)、Write (書き込み) の他に、Delete (消去)、Rename (名称変更)、Execution (実行)、更に全てのアクセスタイプを含む「All」がある。保護対象の名称 401 は、ファイル単位だけでなく、ワイルドカードを用いた複数ファイル指定の他、フォルダ単位やドライブ単位でも指定できる。

【0034】実際にポリシーを設定する際には、情報処理装置 100 を利用する上で必要最小限のアクセスが何であるかを明らかにし、それらを正常アクセスとしてユーザーポリシーに登録することが重要である。また、上記重要度 402 の設定は、仮にそのファイルの内容が不当に改ざんされた場合または、漏洩した場合の被害の大きさを考慮して決めるものである。例えば、パスワードファイルや顧客リストが含まれるファイルには、インターネットから誰でも入手できるようなファイルよりも重要度を高く設定した方がよい。図 4 では、重要度が高いものほど大きい数値を設定している。

【0035】プログラム名 404 には、上記保護対象へのアクセス手段として特別に許可されたプログラムを、当該プログラムファイルのバス名で指定する。特徴値 405 は、上記プログラムファイルがもつ特徴を数値化したものであり、ファイルサイズを指定しても良いし、プログラムファイルのハッシュ値を指定しても良い。これにより、プログラムの不正な改ざんを検知することができる。ユーザー名 406 は、アクセス要求元のプログラムがどのユーザー ID で実行されている場合にアクセスを許可するかを指定する部分である。上記ユーザー名 406 には、ユーザー ID の代わりにグループ ID を指定しても良い。ユーザー ID とグループ ID は、いずれも OS 70 が管理する情報である。

【0036】時間 407 は、アクセスの可否とその時間帯を指定するところであり、例えば 18:00 から 24:00 の間に限りアクセスを許可したい場合は、「+18:00-24:00」と指定する。また、8:00 から 18:00 の間はアクセスを禁止したい場合は、「-08:00-18:00」と指定する。図 4 の例を説明すると、C ドライブの Sec_Proq ディレクトリに含まれるファイル「C:\Sec_Proq*」は全て保護対象であり、その重要度は「2」であることを表す。また、プログラム名が「C:\Sec_Proq\Hsman.exe」であり、且つその特徴値が 0x8A80 であり、且つ上記プログラムがユーザー ID 「sec_admin」の権限で実行されているのであれば、18:00 から 24:00 の時間帯に限り、上記 C:\Sec_Proq ディレクトリ下のファイルに対して「Read (読み出し)」と「Write (書き込み)」を許可することを意味している。

【0037】上記ポリシーの構成要素のうち、重要度 402 と、アクセスタイプ 403、プログラム名 404、特徴値 405、ユーザー名 406、時間 407 については必ずしも全て指定する必要はない。アクセス管理部 80 は、アクセス権チェックの際に指定されていない項目は無視する。以上説明したポリシーは、保護対象毎に正常なアクセスの条件を設定したものである。

【0038】図 16 に、他のポリシー設定例として、プログラム毎にアクセス可能な対象を設定したものを示す。プログラム名 1601 は、アクセス主体となるプログラムをバス名で表したものである。特徴値 1602 は、上記プログラムファイルがもつ特徴を数値化したものであり、図 4 で示した特徴値 405 と同じく、ファイルサイズを指定しても良いし、プログラムファイルのハッシュ値を指定しても良い。ユーザー名 1603 は、上記プログラム名 1601 で指定したプログラムがどのユーザー ID で実行されている場合にアクセスを許可するかを指定する部分である。

【0039】上記ユーザー名 1603 には、図 4 で示したユーザー名 406 と同じく、ユーザー ID の代わりにグループ ID を指定しても良い。アクセスタイプ 1604 では、図 4 で示したアクセスタイプ 403 と同じく、Read (読み出し)、Write (書き込み) の他に、Delete (消去)、Rename (名称変更)、Execution (実行)、更に全てのアクセスタイプを含む「All」から、上記プログラム名 1601 で指定したプログラムが実行可能なアクセスのタイプを選択できる。アクセス対象の名称 1605 は、上記プログラム名 1601 で指定したプログラムがアクセス可能な対象を表すものであり、ファイル単位や、ワイルドカードを用いた複数ファイル指定の他、フォルダ単位、ドライブ単位で指定できる。

【0040】重要度 1607 は、図 4 で示した重要度 402 と同じく、仮にそのアクセス対象が不当に改ざんまたは、漏洩した場合の被害の大きさを考慮して設定するものであり、数値が大きいほど重要度は高い。時間 1606 には、図 4 で示した時間 407 と同じく、アクセスを許可された時間帯を設定する。図 16 の例では、「C:\Sec_Proq\editor.exe」というプログラムの特徴値が「0x3C77」をもち、且つ「users」というユーザー ID もしくはグループ ID で実行されている場合、時間「8:00 から 18:00」の間に限り、「C:\Sec_Proq*.txt」という名称のファイルに対して、Read (読み出し)、Write (書き込み)、Delete (消去) のアクセスが可能となる。

【0041】上記システムポリシー 210 とユーザーポリシー 220 は、上記図 4 で示した形式と図 16 で示した形式のどちらを用いて設定してもよい。

【0042】図 4 で示したポリシーの形式は、情報処理装置 100 における保護対象が何であるかが明確となっていて、その用途を制限したい場合に有効である。これに対して図 16 で示したポリシーの形式は、情報処理装

置100にて利用されるプログラムが明確になっていて、それらプログラムによるアクセス可能な範囲を制限したい場合に有効である。

【0043】ライブラリを動的にリンクしながら機能を拡張できるプログラムを例にとると、図16で示したポリシーの形式を用いて、当該プログラムからリンク可能（Read可能）なライブラリファイルを制限することにより、プログラムの機能を制限することも容易になる。また、特定のライブラリファイルをリンク可能（Read可能）なプログラムを限定したい場合には、図4で示した

10 ポリシーの形式を用いればよい。
【0044】以上説明したポリシー情報に記述されていない保護対象へのアクセスや、同じくポリシー情報に記述されていないプログラムの利用については、全面的に禁止しても良いし、あるいは全て許可しても良い。どちらにするかは、本発明のファイル保護システムを情報処理装置100に導入する際に、情報処理装置100の管理者が決定し、どちらを選択したのかについては、例えば環境設定情報として外部記憶装置40内に保持しておき、アクセス管理部80が参照できるようにしておけば

20 よい。
【0045】図5に、上記エラーコード表230の一例を示す。エラーコード表は、アクセスタイプ501とエラーコード502との対応表である。例えば上記アプリケーションプログラム81から、あるファイルに対するReadアクセスがポリシー違反であった場合、上記アクセス管理部80は、上記エラーコード表230を参照して、エラーコード「0015」をアクセス監視部60を経由して上記アプリケーションプログラム81へ返す。上記エラーコード502には、上記OS70が使用する

30 のものと同じものを登録しておく。
【0046】図7に、上記プロセス情報61の一例を示す。プロセス情報は、現在実行中のプログラムのプロセスID701と、プログラム名702と、ユーザー名703と、特徴値704と、起動日時705からなる。起動日時705は、同一の情報処理装置において過去にOSにより割り当てられ、利用されたプロセスIDが再度利用された場合にも、それらを区別できるように付与する。これらの情報は、プログラムが起動したときに上記アクセス管理部80が取得して登録し、プログラムが終

40 了したときに消去する。なお、本実施例では、実行中のプログラムをプロセス単位で扱っているが、スレッド単位であってもよい。
【0047】図8に、上記ルール情報64を設定するために、上記管理プログラム90が提供するルール設定用グラフィカルユーザーインターフェース（GUI）の一例を示す。当該GUIは、図1に示した表示装置25に表示され、入力装置22を用いて操作できる。情報処理装置100の管理者は、ルール設定用GUI800を操作することで、悪意をもつ不正アクセスかどうかを判別す

るための判定基準810と、当該基準を満たした場合にとるべき防御処理820を設定できる。判定基準810には、例えば、以下に示す3つのタイプを用意し、この中から1つを選択する。

【0048】1つ目のタイプは、重要度Lを割り当てられたファイル、ディレクトリ、またはドライブに対して、一定期間Tにポリシー違反がN回発生した場合に、悪意をもつ不正アクセスと判定するものである。この場合、管理者は図中の重要度指定ラジオボタン812を選択し、上記重要度Lを重要度入力ボックス813に指定し、一定時間Tを有効期間入力ボックス818に指定し、回数Nをポリシー違反回数入力ボックス817に指定する。図に示した例では、重要度3のファイル、ディレクトリ、またはドライブに対して、過去1時間（1h）内に、ポリシー違反が3回以上発生した場合、アクセス元を問わず、アクセス管理部80は、悪意のある不正アクセスと判定する。

【0049】2つ目のタイプは、特定のファイル、ディレクトリ、またはドライブに対して、一定期間Tにポリシー違反がN回発生した場合に、悪意をもつ不正アクセスと判定するものである。この場合、管理者は図中のファイル指定ラジオボタン814を選択し、ファイル名、ディレクトリ名、またはドライブ名を名前入力ボックス815に指定し、一定時間Tを有効期間入力ボックス818に指定し、回数Nをポリシー違反回数入力ボックス817に指定する。図に示した例では、C:\system\passwdというファイルに対して、過去1時間（1h）内に、ポリシー違反が3回以上発生した場合、アクセス元を問わず、アクセス管理部80は、悪意のある不正アクセスと判定する。

【0050】3つ目のタイプは、同一のプロセスから、一定期間Tにポリシー違反がN回発生した場合に、悪意をもつ不正アクセスと判定するものである。この場合、管理者は図中のプロセス指定ラジオボタン816を選択し、一定時間Tを有効期間入力ボックス818に指定し、回数Nをポリシー違反回数入力ボックス817に指定する。図に示した例では、同一のプロセスから、過去1時間（1h）内に、ポリシー違反が3回以上発生した場合、アクセス管理部80は、悪意のある不正アクセスと判定する。

【0051】さらに、上記ルール情報64に複数のルールを登録できるようにして、タイプの異なる判定基準を組み合わせ設定が可能となるように構成しても良い。

【0052】以上の判定基準は、情報処理装置100への侵入者が不正な目的を達成するために、例えばパスワードや、顧客リストが格納された重要なファイルに対して特に重点的にアクセスしてくる可能性が高いといった考えと、コンピュータウィルスに感染したプログラムからは多数のファイルに対して無差別的に不正なアクセスを連続して発行する傾向があるとの考えに基づく。この

ような悪意による不正ファイルアクセスは、ポリシー情報63の設定だけでは防御できない可能性がある。例えばポリシー情報63の設定により保護されていないファイルが存在するケースや、高度な知識をもつ攻撃者が、試行錯誤を繰り返しながら防御機構の抜け穴を見つけるケースである。

【0053】しかし、過失または故意によるポリシー情報63の未設定や防御機構の抜け穴に辿り着くまでには、多くのポリシー違反を繰り返す可能性が非常に高いと予想できる。したがって、上記判定基準を設定することにより、悪意をもつ不正アクセス主体が上記ポリシー情報63の設定ミスや防御機構の抜け穴に辿り着く前に、アクセス管理部80がその兆候を検出することが可能となる。

【0054】次に、上記判定基準が満たされた場合（不正アクセスが発生した場合）に上記アクセス管理部80がとるべき防御処理820の設定方法を示す。防御処理には、例えば以下の3種類あり、このうち2種類以上を組み合わせて指定することもできる。

【0055】1つ目は、ポリシー切り替え処理である。管理者は図中のポリシー切り替え指定チェックボックス821を選択し、切り替え後の新たなポリシーをプルダウンメニュー822から選択して指定する。プルダウンメニュー822には、図3に示したポリシーインデックス200内の、ポリシー名称304からシステムポリシーを除く全てのポリシー名称を、上記アクセス管理部80が読み出して表示する。図に示した例では、上記判定基準を満たした場合、ポリシーを非常モードへ自動的に切り替える。実際に運用モードから非常モードへポリシーを切り替えるには、アクセス管理部80が、上記ポリシーインデックス200中の有効フラグ302を操作し、非常モードの有効フラグを「1」に、運用モードの有効フラグを「0」に書き換える。

【0056】2つ目は、管理者への即時通知である。この場合、管理者は図中の管理者通知指定チェックボックス823を選択し、通知先を宛先アドレス入力ボックス824にて指定する。宛先アドレスは、管理者の電子メールアドレスや、リモートにある管理用ホストのアドレス、あるいは管理者が所持している電話番号でもよい。図に示した例では、上記判定基準が満たされた場合、その旨を管理者の電子メールアドレス(admin@hi-tech.com)に送信する。管理者への通知処理では、アクセス管理部80が、上記通信装置20とネットワーク130を経由して所定のアドレスに対してメッセージを送信する。当該メッセージには、悪意による不正アクセスが発生していると判断した理由（該当する判定基準）と、その対策内容（アクセス管理部80がとるべき防御処理内容）を含める。

【0057】3つ目は、上記判定基準のうち、プロセス指定ラジオボタン816を選択した場合において、当該

判定基準を満たした不正アクセスを行ったプロセス（不正プロセスという）に対する処分である。この場合、管理者は図中の不正プロセスの処分指定チェックボックス825を選択し、更に、下記3つの処分方法の中から1つを選択する。

【0058】ラジオボタン826は、上記不正プロセスによる以後のアクセスを全て禁止するときに指定する。この場合、アクセス管理部80による具体的な処理内容は、上記不正プロセスからのアクセスに対して、アクセス権チェック処理をスキップして、上記ポリシー情報63中のエラーコード表230から該当するエラーコードを読み出し、アクセス監視部60を経由して上記不正プロセスに返す。

【0059】ラジオボタン827は、上記不正プロセスを強制的に終了するときに指定する。この場合、アクセス管理部80は、上記不正プロセスのプロセスIDを指定して上記OS70に対するシステムコールを発行し、プロセスの強制終了を実行する。

【0060】ラジオボタン828は、上記プロセスによる以後のアクセスを、すべてダミーファイルに対するアクセスに変換し、そのアクセスの監視と記録を行うときに指定する。この場合、アクセス管理部80は、上記不正プロセスからのアクセスに対して、アクセス権チェック処理をスキップし、アクセス対象をダミーファイルへと変換し、アクセス監視部60を経由して上記OS70にフォワードする。また、ダミーファイルは上記外部記憶装置40の中に予め用意しておき、そのファイルバス情報をアクセス管理部80が保持しておく。

【0061】最後に、OKボタン830は上記設定内容をルール情報に登録する場合に押すべきボタンであり、キャンセルボタン831は上記設定内容を登録せずにルール設定用GUI800を終了する場合に押すべきボタンである。

【0062】以上のように、設定した判定基準毎にその防御処理を設定できるので、例えば不正なアクセスを受けているファイルの種類や重要度に応じて、通知先のアドレスを変えることも可能となる。

【0063】図9に、上記ルール設定用GUI800を用いて設定されたルール情報64の一例を示す。図中には、構造が同じ3種類のルール（910、920、930）を含んでいる。各ルールは、ルール番号901と、判定基準コード902、重要度3、ファイル名904、ポリシー違反回数905、防御コード906、ポリシー識別番号907、通知先908、プロセスの処分909、有効期間940からなる。

【0064】ルール番号901は、ルール情報64に登録された複数のルールを識別するための番号である。判定基準コード902は、上記ルール設定用GUI800にて、判定基準として何れを選択したかを2進数3桁のビット列で表したものである。重要度指定ラジオボタン

812を選択した場合はビット列「100」、ファイル指定ラジオボタン814を選択した場合はビット列「010」、プロセス指定ラジオボタン816を選択した場合はビット列「001」となる。

【0065】重要度903は、上記判定基準コードのビット列が「100」の場合に登録されるものであり、その他の判定基準コードの場合は空(NULL)とする。ファイル名904は、上記判定基準コードのビット列が「010」の場合に登録されるものであり、その他の判定基準コードの場合は空(NULL)とする。ポリシー違反回数905には、上記ルール設定用GUI800のポリシー違反回数入力ボックス817に指定したものが格納される。防御コード906は、上記ルール設定用GUI800にて、防御処理820に何を選択したかを表すものである。

【0066】防御コード906は、実行すべき防御処理を左から「ポリシー切り替え」、「管理者即時通知」、「不正プロセスの処分」の順に2進数3桁のビット列でコード化したものであり、選択されたものが「1」、選択されていないものが「0」である。ポリシー番号907は、上記ルール設定用GUI800のプルダウンメニュー822にて選択した新たなポリシーの識別番号であり、上記防御コード906のうち、「ポリシー切り替え」が選択されている場合に有効である。通知先908は、上記ルール設定用GUI800の宛先アドレス入力ボックス824にて指定した宛先アドレスであり、上記防御コード906のうち、「管理者即時通知」が選択されている場合に有効である。

【0067】不正プロセスの処分909は、上記ルール設定用GUI800のラジオボタン826～828から選択した結果を2進数3桁のビット列でコード化したものであり、左から「アクセスを全て禁止」、「強制終了」、「アクセス監視と記録」の順に並んでおり、選択されたものが「1」、選択されていないものが「0」である。なお、プロセスの処分909に格納された情報は、上記防御コード906のうち、「不正プロセスの処分」が選択されている場合に有効である。また、有効期間940には、上記ルール設定用GUIの有効期間入力ボックス818に入力した期間Tが登録される。

【0068】図6には、上記ログ情報65の一例を示す。ログ情報には、上記アクセス管理部80により、日時情報610、イベント情報611、イベント内容612といった情報が証跡として書き込まれる。上記イベント内容612には、当該アクセスが正常なアクセスだったのか、ポリシー違反だったのか、どのルール(番号)に該当するポリシー違反だったのか、あるいは不正プロセスによるダミーファイルへのアクセスであったのかを管理者が読んで分かるように記述する。

【0069】また、上記ログ情報65には、下記3種類がある。

【0070】1つは、ファイルアクセスに関する情報であり、図中の601に示すように、日時、イベント、アクセス対象の情報、アクセス発行元の情報から構成される。これにより、いつ、何に、何が、どのようなアクセスを行ったのかが分かる。

【0071】2つ目は、ポリシー切り替えに関する情報であり、図中の602に示すように、日時、イベント、切り替え後のポリシー名、切り替え前のポリシー名から構成される。これにより、いつ、どのポリシーから、どのポリシーへに、切り替えたのかが分かる。

【0072】3つ目は、強制終了されたプロセスに関する情報であり、図中の603に示すように、日時、イベント、プロセス情報から構成される。これにより、いつ、どのプロセスが、強制終了されたのかが分かる。

【0073】図10には、集計情報62の一例を示す。集計情報は、ポリシー違反のアクセスを集計したものであり、ルール番号1001と、ポリシー違反回数1002と、プロセス情報1003、フラグ1004、開始日時1005からなる。ルール番号1001は、上記ルール情報64に登録された各ルールを識別するための情報である。ポリシー違反回数1002は、ルールで指定した有効期間内に発生したポリシー違反回数を、ルール別に集計したものである。プロセス情報1003は、プロセス指定の判定基準を設けたルールに利用されるものであり、ポリシー違反が発生したプログラムの名称やプロセスID、および起動日時を登録する。

【0074】フラグ1004は、上記判定基準を満たしているかどうかを、ルール別に示すものであり、判定基準を満たしている場合、つまり悪意による不正アクセスと思われるものに「1」を設定し、判定基準に達していないものには「0」を設定する。開始日時1005は、ポリシー違反回数のカウントを開始した日時であり、アクセス管理部80が、上記有効期間内に発生したポリシー違反の回数をカウントするために利用する。

【0075】以上説明した各種情報は、例えば図11に示すような情報一覧表示画面1100を、上記管理プログラム90が上記情報処理装置100の表示装置25に表示し、情報処理装置100の管理者の操作を受け付けることによって、管理者は、現在の異常アクセスや不正アクセスの状況を把握したり、入力装置22を操作しながらポリシーを手動で切り替えたりすることが可能となる。

【0076】上記表示画面1100は、ログ情報表示部1101と、当該ログ情報を並べ替えて表示するためのソートボタン1102と、集計情報表示部1103と、プロセス一覧表示部1104と、プロセス終了ボタン1105と、ルール情報表示部1106と、ルール追加ボタン1107と、ルール削除ボタン1108と、ポリシー表示部1109と、ポリシー切り替えボタン1110から構成される。

【0077】上記ログ情報表示部1101は、上記ログ情報65の内容を表示する部分であり、これにより、過去に発生したファイルアクセスや各種イベントの内容を確認できる。ソートボタン1102は、ログ情報を時系列だけでなく、アクセス対象（ファイル）やアクセス主体（プロセス）の名称で並べ替えたり、イベントの種類毎に並べ替えたりするために使われる。

【0078】また、集計情報表示部1103からは、現在悪意による不正アクセスが発生しているかどうかを確認することができる。プロセス一覧表示部1104は、上記プロセス情報61の内容を表示する部分であり、現在実行中のプロセスを確認できる。また、当該表示部1104からプロセスを選択して上記プロセス終了ボタン1105を押すことで、管理者の手動によるプロセス強制終了が可能となる。

【0079】ルール情報表示部1106からは、現在登録されているルール情報64の内容を確認でき、ルール追加ボタン1107を押すことで新規ルールの追加登録もできるし、ルール削除ボタン1108を押すことで、登録済みのルールを削除することもできる。図8に示したルール設定用GUI800は、上記ルール追加ボタン1107を押したときに、管理プログラム90が表示するものである。

【0080】ポリシー表示部1109からは、ポリシー情報63に登録されているポリシーの一覧と、現在選択されているポリシーを確認することができる。また、ポリシー切り替えボタン1110を押すことで、ポリシーを手動で切り替えることもできる。このとき、上記アクセス管理部80が、上記ポリシーインデックス200中の有効フラグ302を書き換えることで、ポリシーが動的に切り替わる。

【0081】以上のような管理者による操作は、セキュリティ上非常に重要であることから、上記管理プログラムの利用に先立って、例えば情報処理装置のOSが備える機能により、管理者の識別と認証処理を実行しておくことが望ましい。

【0082】更に別の管理方法として、図1に示すように、上記管理プログラム90とコマンドやデータを交換する機能と、上記管理プログラム90と同様なユーザーインタフェースとを備えた管理マネージャ91を、ネットワーク130で接続された他の情報処理装置101にて実行し、上記管理者は当該管理マネージャ91が提供するユーザーインタフェースを操作しながら情報処理装置100のログ情報確認や、ルール設定、ポリシーの手動切り替え等をリモートから行うといった実施形態も考えられる。

【0083】図12は、上記アクセス管理部80による、プロセス監視処理内容について示したものである。アクセス管理部80は、一般のアプリケーションプログラム81や管理プログラム90がロードされる前に、主

メモリ50上にロードされ、プロセス情報61を格納するためのテーブルを作成し（ステップ1201）、プロセス監視処理を開始する（ステップ1202）。

【0084】プロセスの起動を検知した場合、ステップ1203にてシステムポリシー210やユーザーポリシー220をチェックして、図4で示したプログラム名404または図16で示したプログラム名1601に記載されていないプログラムのプロセス起動であれば、情報処理装置100の管理者や利用者に対して警告メッセージを表示したり、当該プログラムを強制的に終了したりして、上記ステップ1206の処理をスキップしてプロセス監視処理（ステップ1202）へ戻る。

【0085】上記システムポリシー210やユーザーポリシー220に登録されたプログラムのプロセス起動であれば、当該プロセスに関する情報を上記プロセス情報61のテーブルに格納してから、プロセス監視処理（ステップ1202）へ戻る。

【0086】プロセスの終了を検知した場合、ステップ1204にて、該当するプロセスの情報を上記プロセス情報61のテーブルから削除する。次に、異常アクセス集計情報62に上記プロセスに該当する情報があれば、ステップ1205にて削除し、プロセス監視処理（ステップ1202）へ戻る。

【0087】本実施例では、情報処理装置100にて利用するプログラムを制限するケースを想定してプロセス監視処理を示した。これにより、不正なプログラムの利用を積極的に防止できることから、高いセキュリティを実現できる。ただし、システムポリシー210やユーザーポリシー220には、予め情報処理装置100にて利用可能なプログラムの名称が登録されているものとする。利用するプログラムを特に制限する必要がないのであれば、図12で示したステップ1203の処理を常にスキップすればよい。利用するプログラムの制限の要否については、情報処理装置100の管理者の判断に任せればよい。

【0088】図13は、上記アクセス監視部60とアクセス管理部80によるアクセス監視および不正アクセス対策の処理概要について示したものである。図中のステップ1302と、ステップ1312と、ステップ1313は、アクセス監視部60の処理に含まれる。また、ステップ1303からステップ1311は、アクセス管理部80の処理に含まれる。

【0089】上記アプリケーションプログラム81から上記外部記憶装置40に格納されたファイルへのアクセスが発生すると、アクセス監視部60が当該アクセスを検知し、ステップ1302にて、アクセス対象の名称と、アクセスのタイプと、当該アクセスの発行元となるプロセスIDを上記アクセス管理部80へ通知する。アクセス管理部80では、ステップ1303にて、上記通知されたプロセスIDを手掛かりに、当該プロセスのプ

ログラム名や起動日時をプロセス情報61から取得する。

【0090】次に、ステップ1304では、異常アクセス集計情報62を参照することで、上記プロセスが上記ルール情報にて定義された判定基準を満たす不正プロセスでないことを確認する。ここで、不正プロセスでなければ、ステップ1305のポリシー照合処理に移るが、仮に不正プロセスだった場合には、ステップ1307へジャンプする。ステップ1305のポリシー照合処理の結果、ポリシーに適合した正当なアクセスであればステップ1306にて上記アクセス監視部60に正常リターンを返す。アクセス監視部60は正常リターンを受けると、上記ステップ1312にて、上記アプリケーションプログラム81からのアクセス要求を、OS70へフォワード（転送）する。

【0091】上記ステップ1305のポリシー照合処理の結果、ポリシー違反と判定した場合、ステップ1307にて、アクセス内容をログ情報65に記録する。次にステップ1308では、上記ポリシー違反となったアクセスが、ルール情報64に登録されている何れかのルールに該当する場合、異常アクセス集計情報62へ登録する。具体的には、図10に示したポリシー違反回数1002をインクリメントすると共に、開始日時1005がルールで指定した有効期間内であるかどうかを確認する。

【0092】上記有効期間より古い日時になっている場合には、期限内に発生したポリシー違反を、ログ情報65を参照しながらカウントし直し、上記ポリシー違反回数1002を修正する。同時に、現在の日時から上記有効期間を差し引いた日時を、上記開始日時1005へ登録する。このようなアクセス管理部80による不正アクセス集計処理は、ポリシー違反が発生したタイミングで実行しても良いし、ファイルアクセスとは関係なく定期的に実行するものであっても良い。

【0093】ステップ1309では、上記ポリシー違反のアクセス発生によって、悪意による不正アクセスを判別するための判定基準（ルール情報64に記載されている）に到達するかどうかを判定する。上記判定基準に到達していない場合には、ステップ1311にて、上記ポリシー情報63中のエラーコード表230から該当するエラーコードを取得して、上記アクセス監視部60にリターンする。アクセス監視部60は、上記ポリシー違反のアクセスを発行したアプリケーションプログラム81に対して、上記エラーコードを返し（ステップ1313）、アクセス監視処理に戻る。

【0094】一方、上記判定基準に達した場合には、ステップ1310にてルール情報64に記載されている所定の処理を実行してから、上記アクセス監視部60によるアクセス監視処理に戻る。上記ステップ1310において実行した処理、例えばポリシー切り替えや、管理者

への通知、不正プロセスの強制終了等については、上記ステップ1307と同様にアクセス管理部80がログ情報65に記録しておき、後で管理者によってトレースできるようにする。

【0095】以上説明したファイル保護システムは、ポリシーに違反したアクセスの回数や、アクセス対象の重要度などから、悪意によると思われる不正アクセスをルール情報64に基づいて判定し、且つ対策を実施することができる。つまり、ポリシー情報63に基づくファイルアクセス制御機能だけでなく、侵入やウィルス感染の兆候を不正アクセスのパターンから検出し、早期に対策を実施する機能まで提供することができる。

【0096】図14は、本実施形態のファイル保護システムを搭載した情報処理装置100を用いて構成したインターネット・サイトおよびローカルエリアネットワーク（LAN）の一例を示したものである。インターネットなどの外部ネットワークと内部ネットワークの間には、ファイアウォール140を設置することにより、外部ネットワークから利用可能なエリアであるDMZ（De-Militarized Zone、非武装地帯、）130aに設置された情報処理装置100aが提供するサービスは、インターネット160やLAN130bから利用できるが、インターネット160からLAN130bへのアクセスはできないよう制御できる。

【0097】上記DMZ130aに設置された情報処理装置100aは、例えばWWW（World Wide Web）サーバや、メールサーバ等のインターネットサーバである。また、LAN130bに設置された情報処理装置100bと情報処理装置100cは、それぞれ例えば社内で利用する各種サーバや、業務用の端末装置として利用されるものである。

【0098】ここで、上記DMZ130aに設置された情報処理装置100aにて、例えばセキュリティホール（欠陥）をもつWWWサーバプログラムが動作している場合、当該セキュリティホールが悪用されて情報処理装置100aが侵入され、ホームページの改ざんやパスワードファイルの不正読み出しがなされる可能性がある。このような攻撃には、上記ファイアウォールだけでは対抗しきれないが、本実施形態のファイル保護システムを適用することにより、ユーザーIDだけでなく、アクセス手段となるプログラムや時間帯を制限できるため、侵入された場合にも被害を極小化できる。

【0099】つまり、不正なファイルアクセスを未然に防ぐことができる。しかも、例えばパスワードファイルやホームページのファイルに対してポリシー違反のアクセスが一定時間内に連続して発生した場合に、当該アクセス発行元を強制的に終了するよう上記ルール情報64を設定しておくことで、ファイル保護だけでなく、不正を行う可能性のあるプログラム（プロセス）を積極的に排除することも可能となり、安全なインターネットサー

ビスが提供できるようになる。

【0100】このような不正アクセスは、インターネットだけでなく、社内ネットワーク（LAN130b）などのイントラネットにおいても発生しうる。本実施形態のファイル保護システムを、社内LANの各サーバとなる情報処理装置100bやクライアント（端末）となる情報処理装置100cに適用することで、例えば顧客リストが格納された重要なファイルへのアクセスを監視して漏洩を未然に防いだり、不正なアクセスの発行元となるプロセスを排除したりできる。

【0101】また、ファイルを不正に消去したり、書き込みしたり、あるいは読み出して外部ネットワークへ送信するような悪質なコンピュータウィルスに対しても、そのファイルアクセスの状況から悪意による不正アクセスを検出可能であると共に、ウィルスに感染して不正なファイルアクセスを発行しているプロセスを検出し、強制的に終了させることも可能となる。また、本ファイル保護システムをクライアント（端末）に適用するのであれば、上記管理者への通知用メッセージを、クライアントである情報処理装置100cの表示装置25の画面上にも表示し、利用者に対して警告するものであってもよい。

【0102】更に、上記管理マネージャ91を搭載した情報処理装置101を設置することで、上記DMZ130aやLAN130bに設置された各情報処理装置に対して、リモートからルール設定やアクセス状況の監視、および手動によるポリシー切り替えも可能となる。

【0103】図14には、更に他の適用例として、情報資産の保管場所となる外部記憶装置40を、ストレージ・エリア・ネットワーク（SAN）に置き換えた例も示している。図中のSAN170には、ハードディスクなどの記憶装置を複数台用いて高速、大容量で信頼性の高いディスク装置を実現したRAID（Redundant Arrays of Independent Disks）171や、テープライブラリ172が接続されている。上記情報処理装置100bと各記憶装置（RAID171、テープライブラリ172）との間は、スイッチ175により接続され、例えばファイバチャネル（FC）プロトコルなどを用いてデータ転送を行う。

【0104】この場合、情報処理装置100bはSANのサーバとして、情報処理装置100cから利用される。言い換えれば、SANに接続されている記憶装置を利用するには、必ずSANサーバである情報処理装置100bを経由する。現状、SANのセキュリティ機能には、上記スイッチ175の機能を用いたゾーニングと呼ばれる記憶装置単位のアクセス制御技術と、LUNマスキングと呼ばれるRAID装置内のボリューム単位のアクセス制御技術が確立されている。ただしこれらの技術は、SANのサーバ機器と、各記憶装置あるいはRAIDのボリュームとの間でのアクセス可否を管理するもの

であり、例えば利用者（ユーザーID）毎に、各記憶装置あるいはRAIDの各ボリュームへのアクセス可否を管理するものではない。

【0105】そこで、SANのサーバに本実施形態のファイル保護システムを適用し、記憶装置やボリューム単位での正常なアクセスを、SANサーバである情報処理装置100bのポリシー情報63に記述することで、ユーザーIDやプログラム名を組み合わせたきめ細かなアクセス管理が可能となる。これは、RAID内のファイル単位のアクセスについても勿論同様である。

【0106】このようなポリシー情報を設定するためのポリシー編集画面の一例を図15に示す。図中のポリシー編集画面1500は、上記管理プログラム90あるいは管理マネージャ91が提供するGUIであり、SANのサーバとなる上記情報処理装置100bの表示装置25の画面上、もしくは管理マネージャ91を搭載した情報処理装置101の画面上から管理者が操作するものである。当該編集画面は、保護対象選択部1510、保護対象直接指定部1515、プログラム選択部1520、その他の条件設定部1530からなる。

【0107】上記保護対象選択部1510では、記憶装置単位、ボリューム単位、ディレクトリ単位、ファイル単位で保護対象を表示選択できる。図中の例では、記憶装置「RAID-2」内のボリューム「Vol-1」内のディレクトリ「Doc¥Projects」下にあるファイル「idea.doc」を保護対象として選択している。これにより、ポリシー情報63中の保護対象の名称401には、「RAID-2¥Vol-1¥Doc¥Projects¥idea.doc」が格納される。ただし、上記記憶装置のボリュームが、ある特定のドライブにマッピングしているのであれば、上記管理プログラム90あるいは管理マネージャ91が自動的に当該ドライブ名（例えばD: ¥）に変換して「D:¥Doc¥Projects¥idea.doc」のように設定することも可能である。また、上記記憶装置単位の指定は、RAIDやテープだけでなく、自他問わず情報処理装置が備えている外部記憶装置40も指定可能なものである。

【0108】保護対象直接指定部1515は、保護対象をワイルドカードを用いて複数指定する場合に利用する。図中の例では、「RAID-2¥Vol-1¥Doc¥Projects¥*.doc」と指定されており、これはフォルダ「RAID-2¥Vol-1¥Doc¥Projects」の下にある拡張子が「.doc」のファイル全てを指している。保護対象選択部1510で選択したものと、保護対象直接指定部1515で指定したものが一致しない場合には、保護対象直接指定部1515で指定した方がポリシー情報63中の保護対象の名称401に格納されるように構成すればよい。

【0109】プログラム選択部1520は、上記保護対象に対してアクセスを許可すべきプログラムファイルを選択指定する。図中の例では、「Prog¥office¥Sedit.exe」という名称のプログラムを選択しており、当該プロ

グラム名は、ポリシー情報 63 のプログラム名 404 に格納される。その他の条件設定部 1530 では、保護対象の重要度と、許可すべきアクセスタイプと、ユーザー名/グループ名と、上記プログラムファイルの特徴値と、アクセス可能な時間帯とを指定する。

【0110】このうち特徴値については、プログラム選択部 1520 で選択されたプログラムファイルから、上記管理プログラムが自動的にその特徴値を導出して上記条件設定部 1530 に表示することで、管理者の手間を軽減できる。上記保護対象選択部 1510、プログラム選択部 1520、その他の条件設定部 1530 についてそれぞれ設定した後で OK ボタン 1540 を押すと、設定項目がポリシー情報 63 へ格納される。キャンセルボタン 1541 は、上記設定項目をクリアしたい場合に利用する。ポリシー編集画面 1500 は、例えば図 11 に示した情報一覧表示画面 1100 にボタンを追加し、管理者が当該ボタンを押すことで呼び出し可能なものであっても良い。

【0111】以上説明したように、本実施形態によれば、情報処理装置にて発生するファイルアクセスのうち、ポリシー情報 63 にて規定された正常アクセスに該当しないものを異常アクセスと見なして阻止できると共に、上記異常アクセスから更に悪意による不正アクセスを検出し、且つ防御処理を実行することにより、侵入やウィルス感染等の兆候を素早く検知して、その後予想される被害の発生を抑えることができるという効果がある。

【0112】また、柔軟なルール設定により、過失によるアクセスに対しては過剰な防御処理を不要とし、悪意による不正アクセスに対してのみ防御処理を実行できるという効果がある。特に、手当たり次第にファイルを破壊・削除するような悪質なプログラムを検出して強制終了するなどにより、早期発見から排除まで行えるという効果がある。

【0113】また、本実施形態において、ルール情報に登録しなければ、ポリシー情報に基づくファイルアクセス制御システムとして、セキュリティも重要だが処理スピードも重要視する分野に適用可能であり、ルール情報に登録してセキュリティを最重要視する分野に適用する場合とで、使い分けを行うことも可能である。

【0114】また、ユーザー識別・認証機能とファイルシステムとを備えた OS であれば、本実施形態のファイル保護システムを適用することで容易にセキュリティを強化できる。さらに、ファイアウォールや通信データ暗号機能等のセキュリティ技術と組み合わせることで、ネットワークシステム全体のセキュリティを向上させることができるという効果がある。

【0115】

【発明の効果】本発明によれば、情報処理装置が管理するファイルへの異常アクセスの内、悪意による不正ア

セスを防ぐことが可能になる。

【0116】

【図面の簡単な説明】

【図 1】本発明の実施の形態におけるファイル保護システムの一構成例を示す図。

【図 2】ポリシー情報 63 の一構成例を示す図。

【図 3】各種ポリシーに関するインデックス情報を示す図。

【図 4】ユーザーポリシー 220 の設定の一例を示す図。

【図 5】エラーコード表 230 の一例を示す図。

【図 6】ファイルアクセスや各種イベントを記録するためのログ情報 65 の構造を示す図。

【図 7】現在実行中のプロセスに関する情報を格納したプロセス情報 61 の一例を示す図。

【図 8】ルール情報 64 を設定するための画面の一例を示す図。

【図 9】設定されたルール情報 64 の内部構造を示す図。

【図 10】異常アクセスの集計情報 62 の一例を示す図。

【図 11】管理プログラム 90 が表示装置に表示する管理用画面の一例を示す図。

【図 12】アクセス管理部 80 によるプロセス監視とプロセス情報作成フローを示す図。

【図 13】アクセス監視部 60 とアクセス管理部 80 によるファイルアクセス制御と侵入検知処理のフローチャートを示す図。

【図 14】本実施形態のファイル保護システムを適用したネットワークシステムの一構成例を示す図。

【図 15】ポリシー情報 63 を編集するための画面の一例を示す図。

【図 16】プログラム単位で設定したユーザーポリシー 220 の一例を示す図。

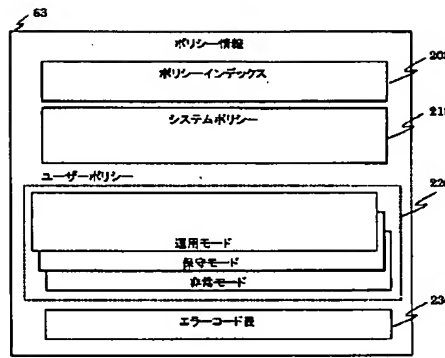
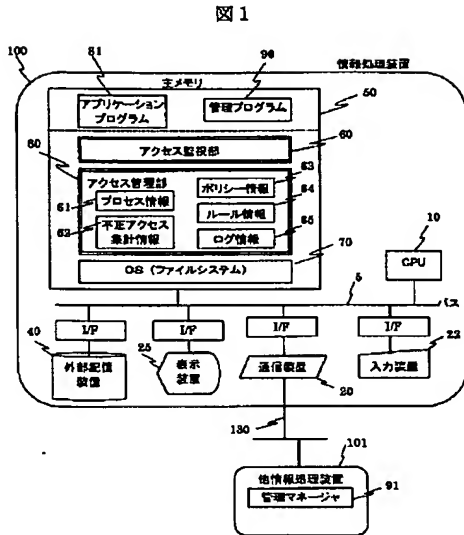
【符号の説明】

5・・・バス、10・・・CPU、20・・・通信装置、22・・・入力装置、25・・・表示装置、40・・・外部記憶装置、50・・・主メモリ、60・・・アクセス監視部、61・・・プロセス情報、62・・・異常アクセス集計情報、63・・・ポリシー情報、64・・・ルール情報、65・・・ログ情報、70・・・OS、80・・・アクセス管理部、81・・・アプリケーションプログラム、90・・・管理プログラム、91・・・管理マネージャ、100・・・情報処理装置、101・・・他の情報処理装置、130・・・ネットワーク、140・・・ファイアウォール、160・・・インターネット、170・・・SAN、171・・・RAID、172・・・テープライブラリ、175・・・スイッチ、200・・・ポリシーインデックス、210・・・システムポリシー、220・・・ユーザーポリシー、230・・・エラーコード表、800・・・ルール情報設定用画面、1100・・・情報一覧表示画面、150

0...ポリシー編集用画面

【図1】

【図2】



【図5】

図5

【図3】

図3

301 デフラグ フラグ	302 有効 フラグ	303 識別番号	304 ポリシー名称	305 ロケーション情報
1	1	0000	システムポリシー	1 - 20
1	0	1010	運用モード	20 - 80
0	1	1020	保守モード	35 - 65
0	0	1030	非常モード	60 - 88

200 ポリシーインデックス

エラーコード表	
アクセスタイプ	エラーコード
Read	0015
Write	0018
Delete	0021
Rename	0024
Execute	0030
All	0050

【図4】

220 保護対象の名称	401 重要度	403 アクセスタイプ						404 プログラム名	405 特徴値	406 ユーザー名	407 時間
		A	X	N	D	W	R				
C:\Sec_Prog*	2						*	c:\prog\Haman.exe	0x8A80	sec_admin	+18:00-24:00
C:\Prog*	1	*						c:\prog\Haman.exe	0x8A80	sec_admin	+00:00-24:00
C:\Prog\Way*	1	*						c:\prog\Haman.exe	0x8A80	sec_admin	-08:00-18:00
D:\Doc*	3	*						c:\prog\Haman.exe	0x8A80	sec_admin	+00:00-24:00

A: All
X: Execute
N: Rename
D: Delete
W: Write
R: Read

図4

【図6】

図6

ログ情報

日時	イベント	アクセス対象の情報	アクセス発行元の情報
日時	イベント	切り替え後のポリシー	切り替え前のポリシー
日時	イベント	強制終了されたプロセスの情報	

【図7】

図7

プロセスID	プログラム名	ユーザー名	特徴値	起動日時

【図9】

図9

ルール情報

ルール番号	001
判定基準コード	100
重要度	3
ファイル名	
ポリシー違反回数	3
防御コード	110
ポリシー識別番号	1030
通知先	admin@hi-tech.com
プロセスの区分	
有効期間	60min

ルール番号	002
判定基準コード	010
重要度	
ファイル名	C:\system\passwd
ポリシー違反回数	3
防御コード	110
ポリシー識別番号	1030
通知先	admin@hi-tech.com
プロセスの区分	
有効期間	60min

ルール番号	003
判定基準コード	001
重要度	
ファイル名	
ポリシー違反回数	3
防御コード	011
ポリシー識別番号	
通知先	admin@hi-tech.com
プロセスの区分	001
有効期間	60min

【図8】

図8

ルールの設定

判定基準の設定

タイプを選択

重要度指定
重要度 3

ファイル指定
C:\system\passwd

プロセス指定

ポリシー違反回数 3

有効期間 1h

防御処理

☒ ポリシー切り替え
ポリシー 非常モード

☒ 管理者即時通知 宛先アドレス admin@hi-tech.com

☐ 不正プロセスの処分

826 ☒ アクセスを全て禁止
827 ☐ 強制終了
828 ☐ アクセス監視と記録

OK キャンセル

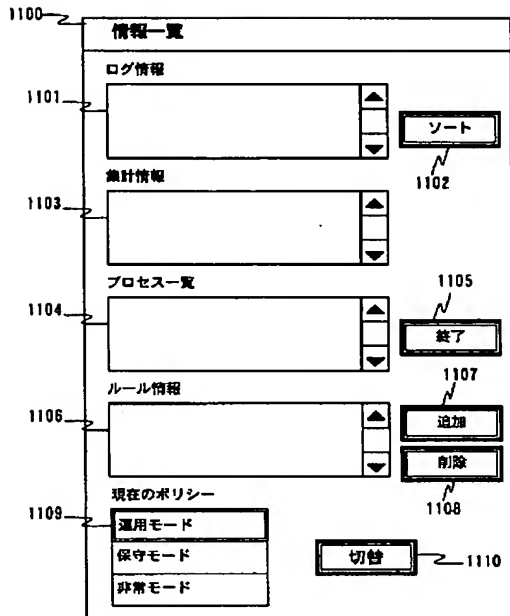
【図10】

図10

ルール番号	ポリシー違反回数	アクセス主体	フラグ	開始日時
001	1		0	10:21
003	3	プログラム名 プロセスID	1	09:55
002	2		0	10:05

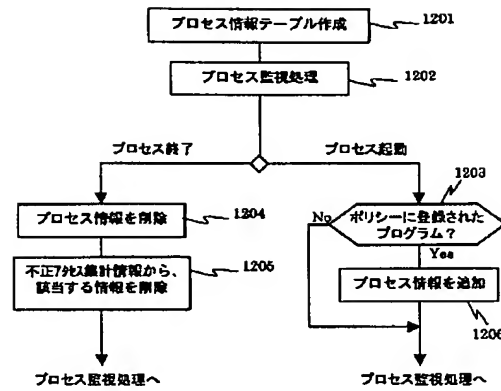
【図11】

図11



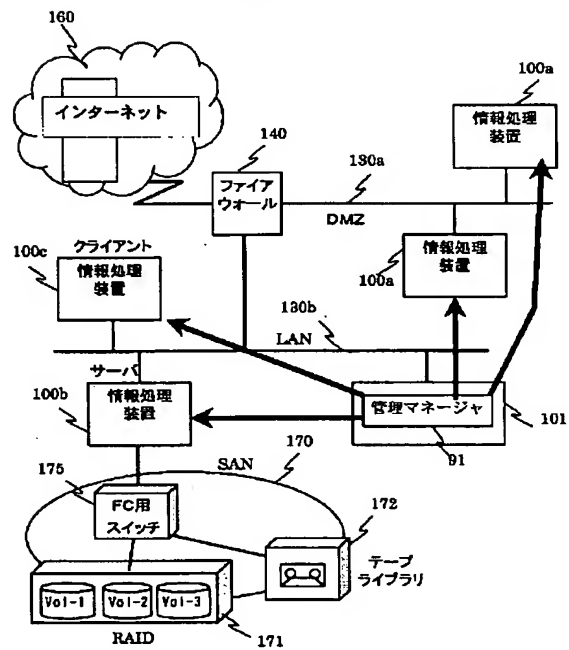
【図12】

図12



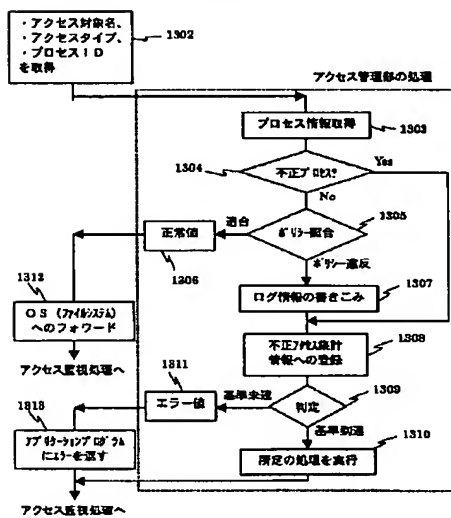
【図14】

図14



【図13】

図13



【図15】

図15

1500

ポリシー編集

1510

1515

1520

1530

1540

1641

ファイル名	サイズ	更新日時
Common.txt	2KB	30/9/00
idea.doc	2KB	4/10/00
present.doc	4KB	1/11/01

RAID-1

RAID-2

Val-1

Doc

Projects

RAID2 Val-1 Doc Projects w.doc

Prog

comm

office

plus-in

プログラム名

viewer.exe

3edit.exe

present.exe

html_edit.exe

重要度	アクセス	ユーザー	特徴値	時間
3	<input checked="" type="checkbox"/> R <input checked="" type="checkbox"/> W <input type="checkbox"/> A	Alex	0x8880	開始 終了 00:00 18:00

OK

キャンセル

【図16】

220	1601	1602	1603	1604	1605	1606	1607	1608			
プログラム名	特徴値	ユーザー名	アクセスタイプ						アクセス対象の名称	重要度	時間
			A	X	N	D	W	R			
C:\sys\Loader.exe	0x09B1	admin						*	C:\sys*.dll	1	+00:00-24:00
C:\sys\Loader.exe	0x09B1	admin						*	C:\sys*.dll	1	+00:00-24:00
C:\prog\editor.exe	0x3C77	users				*	*	*	C:\users*.txt	2	+08:00-18:00

A: All
 X: Execute
 N: Rename
 D: Delete
 W: Write
 R: Read

図 16

フロントページの続き

Fターム(参考) 5B017 AA03 BA06 CA07 CA16
5B076 FB03
5B082 EA11